Discrete Mathematics 18 (1977) 179–211.

THE WEIGHT DISTRIBUTION OF IRREDUCIBLE CYCLIC CODES WITH BLOCK LENGTHS $n_1((q^l - 1)/N)$

Tor HELLESETH, Torleiv KLØVE
and Johannes MYKKELTVEIT
Universitetet I Bergen, Matematisk Institutt, AVD. A, 5014 Bergen-Universitetet, Norway

Received 18 July 1975
Revised 20 April 1976

We study the weight distribution of irreducible cyclic (n, k) codes with block lengths $n = n_1((q^l - 1)/N)$, where $N \mid q - 1$, $\gcd(n_1, N) = 1$, and $\gcd(l, N) = 1$. We present the weight enumerator polynomial, $A(z)$, when $k = n_1 l$, $k = (n_1 - 1)l$, and $k = 2l$. We also show how to find $A(z)$ in general by studying the generator matrix of an (n_1, m) linear code, V_2^*, over $GF(q^d)$ where $d = \gcd(\mathrm{ord}_{n_1}(q), l)$. Specifically we study $A(z)$ when V_2^* is a maximum distance separable code, a maximal shiftregister code, and a semiprimitive code. We tabulate some numbers A_w which completely determine the weight distribution of any irreducible cyclic $(n_1(2^l - 1), k)$ code over GF(2) for all $n_1 \leq 17$.

1. Introduction

In this paper we want to study irreducible cyclic codes over $GF(q)$ with block lengths $n = n_1(q^l - 1)$. We begin by giving a definition of an irreducible cyclic code.

Definition 1.1. Let $h(x) \in GF(q)[x]$ be an irreducible polynomial of degree k and period n. *An irreducible cyclic (n, k) code* V over $GF(q)$ is then defined by

$$V = \{v(c) \mid v(c) = (\mathrm{Tr}_1^k(c), \mathrm{Tr}_1^k(c\beta), \ldots, \mathrm{Tr}_1^k(c\beta^{n-1})), c \in GF(q^k)\}$$

where β is root of $h(x)$. (Here k is the multiplicative order of $q \pmod n$.)

The problem of finding the weight enumerator polynomials for irreducible cyclic codes has been studied by many authors. Few general results have been obtained.

In [4] Delsarte and Goethals found an infinite class of irreducible binary cyclic codes in which only two weights occurred, and which contained a class of two-weight codes discovered by McEliece [5].

In [1] Baumert and McEliece generalized these results by showing the existence of irreducible cyclic two-weight codes over $GF(q)$.

McEliece and Rumsey [7] studied the weight distribution of irreducible cyclic codes by using earlier results on Gaussian sums. Let $N = ((p^k - 1)/n)$ be the number of nonzero cycles in the irreducible code. They constructed an infinite sequence of irreducible cyclic codes which had the same N. The weight distribution

of the irreducible cyclic codes in this sequence could be found from the knowledge of the shortest cyclic code in the sequence.

The weight enumerator for irreducible cyclic codes has been determined in the following cases.

(1) When $N \mid p^j + 1$ for some $j > 0$ then we get a class of two-weight codes, see Baumert and McEliece [1].

(2) For $N = 2$ the weight distribution is found by Baumert and McEliece [1].

(3) For $N = 3$ and $N = 4$ the weight distribution is found by Mykkeltveit (unpublished).

(4) For N a prime, $N \equiv 3 \pmod 4$, and $\mathrm{ord}_p(N) = (N-1)/2$, the weight distribution is due to Baumert and Mykkeltveit [2].

In [6] McEliece extended these results to GF(q). He also proved that the results are true when N is replaced by $N_1 = \gcd((q^k - 1)/n, (q^k - 1)/(q-1))$.

In this paper we will construct an infinite sequence of irreducible cyclic codes over GF(q), with block lengths $n = n_1(q^l - 1)$, where n_1 and $d = \gcd(\mathrm{ord}_{n_1}(q), l)$ are fixed. Note that the number of cycles will not be constant in these sequences.

We will show that if the weight enumerator polynomial for an arbitrary $(n, k) = (n_1(q^l - 1), ml)$ code V in this sequence is $A(z)$ then $A(z) = A^*(z^{q^{l-1}(q-1)})$, where $A^*(z)$ is the weight enumerator polynomial of an (n_1, m) code V^* over GF(q^l) (Lemma 2.4). A similar result is proved by Goethals [8] when $\gcd(n_1, q^l - 1) = 1$.

The main goal with this paper is to show that (Corollary 4.4, Lemma 4.5, Theorem 4.6, and Corollary 4.7):

(a) V^* is the direct sum of e copies of an $(n_1/e, m/e)$ code $V_1^{*\prime}$ over GF(q^l), and thus $A^*(z) = (A^{*\prime}(z))^e$, for some integer e dividing $\gcd(n_1, m)$.

(b) $A^{*\prime}(z)$ is determined by some integers A_{ij}, $i = 0, 1, \ldots, n_1/e$, $j = 0, 1, \ldots, m/e$ which only depend on the generator matrix for the code $V_2^{*\prime}$.

Thus we reduce the problem of finding the weight enumerator polynomials for the infinite sequence of codes to the problem of finding $((n_1/e)+1)((m/e)+1)$ numbers A_{ij}.

2. Some basic results

In this section we present some results which will be useful later. We also give the weight enumerators for three infinite classes of irreducible cyclic codes.

Lemma 2.1. *Let*

$$V = \{v(c) \mid v(c) = (\mathrm{Tr}_1^k(c), \mathrm{Tr}_1^k(c\beta), \ldots, \mathrm{Tr}_1^k(c\beta^{n-1})), c \in \mathrm{GF}(q^k)\}$$

be an irreducible cyclic code over GF(q). *Let* $n = n_1 n_2$ *where* $n_2 \mid q^l - 1$. *Then the components of* $v(c)$ *can be arranged as an* $n_1 \times n_2$ *matrix* $(u_{i_1 i_2})$ *such that* $u_{i_1 i_2} = \mathrm{Tr}_1^l(\beta^{i_2 n_1} \mathrm{Tr}_l^k(c\beta^{i_1}))$.

Proof. Let $0 \leq j < n$. Then j can be written uniquely as $j = j_2 n_1 + j_1$ with $0 \leq j_1 < n_1$ and $0 \leq j_2 < n_2$. Let $v_j(c)$ denote the jth component in $v(c)$. Then

$$\begin{aligned} v_j(c) &= \mathrm{Tr}_1^k(c\beta^j) \\ &= \mathrm{Tr}_1^k(c\beta^{j_2 n_1 + j_1}) \\ &= \mathrm{Tr}_1^k(\beta^{j_2 n_1} c\beta^{j_1}). \end{aligned}$$

Since $\beta^{n_1 n_2} = 1$ we have $\beta^{j_2 n_1} \in \mathrm{GF}(q^l)$. Therefore

$$\begin{aligned} v_j(c) &= \mathrm{Tr}_1^l(\beta^{j_2 n_1} \mathrm{Tr}_l^k(c\beta^{j_1})) \\ &= u_{j_1 j_2}. \end{aligned}$$

Corollary 2.2. *Let $n = n_1 n_2$ where $n_2 \mid q^l - 1$ and l is as small as possible. Then each row-vector belongs to an irreducible cyclic (n_2, l) code.*

In particular, if $n_2 = q^l - 1$, thus $k = ml$, then each row-vector belongs to a maximal shift-register code.

From now on we assume that $n_2 = q^l - 1$. We will use the following notations:

$$V = \{v(c) \mid v(c) = (\mathrm{Tr}_1^k(c), \mathrm{Tr}_1^k(c\beta), \ldots, \mathrm{Tr}_1^k(c\beta^{n-1})), c \in \mathrm{GF}(q^k)\},$$

$$V^* = \{v^*(c) \mid v^*(c) = (\mathrm{Tr}_l^k(c), \mathrm{Tr}_l^k(c\beta), \ldots, \mathrm{Tr}_l^k(c\beta^{n_1-1})), c \in \mathrm{GF}(q^k)\},$$

$$V^{*+} = \{v^{*+}(c) \mid v^{*+}(c) = (\mathrm{Tr}_l^k(c), \mathrm{Tr}_l^k(c\beta), \ldots, \mathrm{Tr}_l^k(c\beta^{n-1}), c \in \mathrm{GF}(q^k)\}.$$

We note that:
V is an irreducible cyclic (n, k) code over $\mathrm{GF}(q)$,
V^* is a linear $(n_1, k/l)$ code over $\mathrm{GF}(q^l)$, and
V^{*+} is an irreducible cyclic $(n_1(q^l - 1), k/l)$ code over $\mathrm{GF}(q^l)$.

Lemma 2.3. *Let $v^{*+} = (v_0, v_1, \ldots, v_{n-1}) \in V^{*+}$. Then $v_{sn_1+t} = \beta^{n_1 s} v_t$.*

Proof. From the definition of V^{*+} we get

$$v_{sn_1+t} = \mathrm{Tr}_l^k(c\beta^{sn_1+t}) = \beta^{sn_1} \mathrm{Tr}_l^k(c\beta^t) = \beta^{sn_1} v_t$$

since $\beta^{n_1} \in \mathrm{GF}(q^l)$.

Lemma 2.4. *Let $A(z), A^*(z), A^{*+}(z)$ denote the weight enumerators of V, V^*, V^{*+} respectively. Then*

$$A(z) = A^*(z^{q^{l-1}(q-1)}) = A^{*+}(z^{q^{l-1}(q-1)/(q^l-1)}).$$

Proof. Let $A^*(z) = \sum_{i=0}^{n_1} A_i^* z^i$. We have a one-to-one correspondence between V^* and V given by $v^*(c) \leftrightarrow v(c)$. Let i be the weight of $v^*(c)$. According to Corollary 2.2 the weight of $v(c)$ is $q^{l-1}(q-1)i$ since i rows are nonzero and $q^{l-1}(q-1)$ is the weight of a nonzero codeword in a maximal shift register code.

Therefore by definition we get

$$A(z) = \sum_{i=0}^{n_1} A_i^* z^{q^{l-1}(q-1)i} = A^*(z^{q^{l-1}(q-1)}) = A^{*+}(z^{q^{l-1}(q-1)/(q^l-1)})$$

since $A^{*+}(z) = A^*(z^{q^l-1})$. We always have $1 \leq k/l \leq n_1$.

Theorem 2.5. *Let V be an irreducible cyclic $(n_1(q^l-1), k)$ code over* GF(q). *If $k/l = n_1$, then*

$$A(z) = (1 + (q^l - 1)z^{q^{l-1}(q-1)})^{n_1}.$$

Proof. Since $k/l = n_1$, V^* is an (n_1, n_1) code. Therefore

$$A^*(z) = \sum_{i=0}^{n_1} \binom{n_1}{i} (q^l-1)^i z^i = (1 + (q^l-1)z)^{n_1}.$$

The theorem now follows from Lemma 2.4.

Theorem 2.6. *Let V be an irreducible cyclic $(n_1(q^l-1), k)$ code over* GF(q). *If $k/l = n_1 - 1$, then*

$$A(z) = \sum_{i=0}^{n_1} \binom{n_1}{i} \frac{(q^l-1)^i + (q^l-1)(-1)^i}{q^l} z^{q^{l-1}(q-1)i}.$$

Proof. Since $k/l = n_1 - 1$, V^* is an $(n_1, n_1 - 1)$ linear code. By Lemma 2.3 the parity check polynomial $H(x)$ of V^{*+} must divide $x^{n_1} - \beta^{n_1}$. We have $x^{n_1} - \beta^{n_1} = \prod_{i=0}^{n_1-1}(x - \alpha^i\beta)$ where α is a primitive n_1th root of unity. Since $H(x)$ has degree $n_1 - 1$ we have $H(x) = ((x^{n_1} - \beta^{n_1})/(x - \alpha^a\beta))$ for some a such that $\alpha^a\beta \in$ GF(q^l). Therefore

$$H(x) = \frac{x^{n_1} - \delta^{n_1}}{x - \delta} = x^{n_1-1} + \delta x^{n_1-2} + \cdots + \delta^{n_1-1}$$

for $\delta = \alpha^a\beta$. Since V^* consists of the first n_1-tuple of the codewords in V^{*+}, which has $H(x)$ as parity check polynomial, then V^* is an $(n_1, n_1 - 1)$ code.

The dual code V_1^* of V^* is an $(n_1, 1)$ code, and $(\delta^{n_1-1}, \ldots, \delta, 1)$ is a codeword in the dual code. Therefore

$$V_1^* = \{\gamma(\delta^{n_1-1}, \ldots, \delta, 1) \mid \gamma \in \text{GF}(q^l)\}.$$

Let $B^*(z)$ denote the weight enumerator of V_1^*. Then $B^*(z) = 1 + (q^l - 1)z^{n_1}$. Using MacWilliams identities we get

$$\begin{aligned} q^l A^*(z) &= (1 + (q^l-1)z)^{n_1} B^*\left(\frac{1-z}{1+(q^l-1)z}\right) \\ &= (1 + (q^l-1)z)^{n_1} + (q^l-1)(1-z)^{n_1} \\ &= \sum_{i=0}^{n_1} \binom{n_1}{i} ((q^l-1)^i + (q^l-1)(-1)^i) z^i. \end{aligned}$$

We now apply Lemma 2.4 and get the desired result.

In Theorem A.3 we find the values of n_1 and l for which $k/l = n_1$ or $k/l = n_1 - 1$.

Example. Let V be an (35, 12) irreducible binary code. We put $n_1 = 5$, $l = 3$. Then $k/l = 4 = n_1 - 1$, and we can apply Theorem 2.6 to get

$$A(z) = \sum_{i=0}^{5} \binom{5}{i} \left(\frac{7^i + 7(-1)^i}{8}\right) z^{4i}$$

$$= 1 + 70z^8 + 420z^{12} + 1505z^{16} + 2100z^{20}.$$

This agrees with Table 16.1 in Berlekamp [3].

Theorem 2.7. *Let V be an $(n_1(q^l-1), k)$ irreducible cyclic code over GF(q). If $k/l = 2$, then the weight enumerator of V is*

$$A(z) = 1 + (q^l - 1)n_1 z^{q^{l-1}(q-1)(n_1-1)} + (q^{2l} - 1 - (q^l - 1)n_1) z^{q^{l-1}(q-1)n_1}.$$

Proof. By Lemma 2.4 it is sufficient to prove that $V^* - \{0\}$ has no codewords of weight less than $n_1 - 1$, and to find the number of codewords of weight $n_1 - 1$.

Suppose $v^*(c) = (v_0, \ldots, v_{n_1-1})$ has $v_j = 0$ and $v_{j+s} = 0$ for some $s > 0$. We want to show that this leads to a contradiction. Let $v^{*+}(c) = (v_0, \ldots, v_{n-1})$. Choose t such that $\beta^{n_1 t} = v_{j+1}^{-1} v_{j+s+1}$, and $0 < t \leq q^l - 1$. This is possible since β^{n_1} is a primitive element of GF(q^l). By Lemma 2.3 we have

$$(v_{j+n_1 t}, v_{j+n_1 t+1}) = (\beta^{n_1 t} v_j, \beta^{n_1 t} v_{j+s})$$

$$= (0, v_{j+s+1})$$

$$= (v_{j+s}, v_{j+s+1}).$$

Since dim $V^{*+} = 2$, this means that $v^{*+}(c)$ has period ε where $\varepsilon \leq n_1 t - s < n_1 t \leq n_1(q^l - 1)$. This is impossible since V^{*+} is an $(n_1(q^l - 1), 2)$ irreducible cyclic code.

Since V^{*+} is cyclic and V^* has period n_1 we have

$$A^*_{n_1-1} = n_1 |\{v \in V^{*+} - \{0\} \mid v_0 = 0\}| = n_1(q^l - 1).$$

By Lemma 2.4,

$$A(z) = 1 + (q^l - 1)n_1 z^{q^{l-1}(q-1)(n_1-1)} + (q^{2l} - 1 - (q^l - 1)n_1) z^{q^{l-1}(q-1)n_1}.$$

Since

$$N = \frac{q^{2l} - 1}{n_1(q^l - 1)} = \frac{q^l + 1}{n_1} \mid q^l + 1,$$

Theorem 2.7 is a special case of a theorem of Baumert and McEliece [1] which they proved by other methods.

3. Codes with related generator matrices

In this section we will study some infinite sequences of linear codes which have related generator matrices. All of the codes in the sequence are (n, m) codes, and the lth code has codewords from $\mathrm{GF}(q^l)^n$. In the following sections we will apply the results in this section and get some results on the weight distribution of irreducible cyclic codes. We will here, however, formulate and prove the results for linear codes in general.

Lemma 3.1. *Let $X_l = \mathrm{GF}(q^l)^m$. Let F denote the family of subspaces of X_1. For $U \in F$ define K_U by*

$$K_U = \{x \in X_l \mid x \cdot u = 0 \iff u \in U\}.$$

Then

(i) $\bigcup_{U \in F} K_U = X_l$.

(ii) *If $U_1, U_2 \in F$ and $U_1 \neq U_2$, then $K_{U_1} \cap K_{U_2} = \emptyset$.*

(iii) *Let G be an $m \times n$ matrix over $\mathrm{GF}(q)$, and let g_i denote the ith column of G. Let $U \in F$ and $x \in K_U$. Then $w(xG) = n - |\{t \mid g_t \in U\}|$. We write $w(G, U)$ for this number.*

(iv) $|K_U| = \prod_{i=0}^{m-\dim U-1} (q^l - q^i)$.

Proof. (i) By definition $K_U \subseteq X_l$ for $U \in F$. Let $x \in X_l$. Define $U_x = \{u \in X_1 \mid x \cdot u = 0\}$. Then $U_x \in F$ and $x \in K_{U_x}$. Therefore $X_l \subseteq \bigcup_{U \in F} K_U$.

(ii) Suppose $x \in K_{U_1} \cap K_{U_2}$. Let $u_1 \in U_1$. Then since $x \in K_{U_1}$ we have $x \cdot u_1 = 0$. Since $x \in K_{U_2}$ and $x \cdot u_1 = 0$, $u_1 \in U_2$. Hence $U_1 \subseteq U_2$. By symmetry $U_1 = U_2$ which is a contradiction. Therefore $K_{U_1} \cap K_{U_2} = \emptyset$ when $U_1 \neq U_2$.

(iii) Let $x \in K_U$. Let $a = xG$. Then $a_i = x \cdot g_i$. Hence $a_i = 0$ if and only if $g_i \in U$. That is,

$$w(xG) = n - |\{t \mid g_t \in U\}|.$$

Therefore $w(xG)$ only depends on U and G.

(iv) Let $U \in F$, $\dim U = m - j$. Let

$$B = \{v_1, v_2, \ldots, v_j, v_{j+1}, \ldots, v_m\}$$

be a basis for X_1 such that $\{v_{j+1}, \ldots, v_m\}$ is a basis for U. Considered as a subset of X_l, B is a basis for X_l. Let $\{v_1^*, \ldots, v_m^*\}$ be a basis dual of the basis B, i.e. such that $v_i \cdot v_j^* = \delta_{ij}$. Then $x = \sum_{i=1}^m x_i v_i^* \in K_U$ if and only if $x_i = 0$ for $i = j+1, j+2, \ldots, m$ and $\sum_{i=1}^l \alpha_i x_i \neq 0$ for all $(\alpha_1, \ldots, \alpha_l) \in \mathrm{GF}(q)^l \setminus \{(0, \ldots, 0)\}$. If we choose $x_1, x_2, \ldots, x_j$ one at the time there are $q^l - 1$ choices for x_1 since $x_1 \neq 0$. There are $q^l - q$ choices for x_2 since $x_2 + \alpha_1 x_1 \neq 0$ for all $\alpha_1 \in \mathrm{GF}(q)$, etc. Hence the total number of choices for $(x_1, \ldots, x_j)$ to make $x \in K_U$ is $\prod_{i=0}^{j-1} (q^l - q^i)$.

Theorem 3.2. *Let $G = (g_{ij})$ be an $m \times n$ matrix where $g_{ij} \in \mathrm{GF}(q)$. Let $G_l = (g_{ij}^{(l)})$*

where $g_{ij}^{(l)} = \delta_j g_{ij}$ for some $\delta_j \in \mathrm{GF}(q^l)\backslash\{0\}$. Let $V_l = \{xG_l \mid x \in X_{n_1}\}$ be an (n, m) linear code over $\mathrm{GF}(q^l)$. Let $A_l(z)$ denote the weight enumerator of V_l. Then

$$A_l(z) = \sum_{i=0}^{n} \sum_{j=0}^{m} A_{ij}(q^l-1)(q^l-q)\cdots(q^l-q^{j-1})z^i,$$

where A_{ij} is the number of $(m-j)$-dimensional subspaces of X_{n_1} which contain exactly $n-i$ of the n column vectors of G.

Proof. Let g_j denote the jth column of G. Then $\delta_j g_j$ is the jth column of G_l. We then have $w(xG_l) = w(xG)$ for $x \in X_{n_1}$ since $x \cdot g_j = 0$ if and only if $x \cdot \delta_j g_j = 0$.

By definition and by Lemma 3.1 we have,

$$\begin{aligned}
A_l(z) &= \sum_{x \in X_{n_1}} z^{w(xG_l)} \\
&= \sum_{x \in X_{n_1}} z^{w(xG)} \\
&= \sum_{U \in F} \sum_{x \in K_U} z^{w(xG)} \\
&= \sum_{U \in F} |K_U| z^{w(G,U)} \\
&= \sum_{i=0}^{n} z^i \sum_{\substack{U \in F \\ w(G,U)=i}} |K_U| \\
&= \sum_{i=0}^{n} z^i \sum_{j=0}^{m} (q^l-1)(q^l-q)\cdots(q^l-q^{j-1}) \sum_{\substack{U \in F \\ w(G,U)=i \\ \dim U = m-j}} 1.
\end{aligned}$$

Corollary 3.3. *For $j = 0, 1, \ldots, m$ we have*

$$\sum_{i=0}^{n} A_{ij} = \prod_{i=0}^{j-1} \frac{q^m - q^i}{q^j - q^i}.$$

Proof. By Theorem 3.2 we have

$$\sum_{i=0}^{n} A_{ij} = \sum_{i=0}^{n} |\{U \in F \mid \dim U = m-j, w(G,U) = i\}| = |\{U \in F \mid \dim U = m-j\}|.$$

Hence $\sum_{i=0}^{n} A_{ij}$ is the number of $(m-j)$-dimensional subspaces of an m-dimensional vectorspace over $\mathrm{GF}(q)$, which is equal to $\prod_{i=0}^{j-1}((q^m-q^i)/(q^j-q^i))$ according to Berlekamp [3, p. 261].

4. Chains of irreducible cyclic codes

Let $r = \mathrm{ord}_{n_1}(q)$, $m = \mathrm{ord}_{n_1((q^l-1)}(q^l)$, and $d = \gcd(\mathrm{ord}_{n_1}(q), l)$, and let G_1^* and G_2^* denote the generator matrices of V_1^* and V_2^* respectively. When $\gcd(n_1,$

$(q^l - 1)/(q^d - 1)) = 1$, we show that G_l^* and G_d^* are related as in Theorem 3.2, so that we can obtain the weight enumerator polynomial of V_l^* considering G_d^* only. When $\gcd(n_1, (q^l - 1)/(q^d - 1)) > 1$, we show that G_l^* is related to the direct sum of copies of $G_{d'}^*$ for some d', for which we can apply Theorem 3.2 and obtain the weight enumerator polynomial of V_l^*.

Lemma 4.1. *If* $\gcd(a, b) = 1$, $b \mid c$, *and* $c \neq 0$ *then there exists a* t *such that* $\gcd(at + b, c) = 1$.

Proof. Let $N = \prod_{p \mid c, p \nmid a} p$. Choose t such that $at + b \equiv 1 \pmod N$. Suppose $p \mid \gcd(at + b, c)$. Then $p \mid c$ and $p \nmid N$. Therefore $p \mid a$ which gives that $p \nmid b$. Hence $p \nmid at + b$, a contradiction.

Theorem 4.2. *Let* V_d^{*+} *be an irreducible cyclic* $(n_1(q^d - 1), m)$ *code over* $\mathrm{GF}(q^d)$ *with generator matrix*

$$G_d^{*+} = [1, \beta, \beta^2, \ldots, \beta^{n_1(q^d-1)-1}].$$

If $d = \gcd(\mathrm{ord}_{n_1}(q), l)$ *and* $\gcd(n_1, (q^l - 1)/(q^d - 1)) = 1$, *then there exists an element* δ *of* $\mathrm{GF}(q^l)$ *such that the code with generator matrix*

$$G_l^{*+} = [1, \delta\beta, \delta^2\beta^2, \ldots, \delta^{(q^l-1)-1}\beta^{n_1(q^l-1)-1}]$$

is an irreducible cyclic $(n_1(q^l - 1), m)$ *code over* $\mathrm{GF}(q^l)$.

Remark. Note that we regard G_d^{*+} and G_l^{*+} as $m \times n_1(q^d - 1)$ and $m \times n_1(q^l - 1)$ matrices over $\mathrm{GF}(q^d)$ and $\mathrm{GF}(q^l)$ respectively.

Proof. Since the order of β is $n_1(q^d - 1)$, β^{n_1} is a primitive root of $\mathrm{GF}(q^d)$. Choose a primitive root ψ of $\mathrm{GF}(q^l)$ such that $\beta^{n_1} = \psi^{(q^l-1)/(q^d-1)}$ and choose t such that $\gcd(n_1 t + (q^l - 1)/(q^d - 1), q^l - 1) = 1$. This is possible by Lemma 4.1. Put $\delta = \psi^t$. According to Lemma A.2 it is sufficient to show that $\delta\beta$ is an element of order $n_1(q^l - 1)$.

Suppose $(\delta\beta)^r = 1$. Then $\delta^{m_1}\beta^{m_1} = 1$ and therefore $\psi^{r(n_1 t + (q^l-1)/(q^d-1))} = 1$. Since $\gcd(n_1 t + (q^l - 1)/(q^d - 1), q^l - 1) = 1$ we get $r \equiv 0 \pmod{q^l - 1}$. Put $r = a(q^l - 1)$. We have $\delta^{a(q^l-1)}\beta^{a(q^l-1)} = 1$ which means that $\beta^{a(q^l-1)} = 1$. Therefore $a(q^l - 1) \equiv 0 \pmod{n_1(q^d - 1)}$ and so $a(q^l - 1)/(q^d - 1) \equiv 0 \pmod{n_1}$. Since $\gcd(n_1, (q^l - 1)/(q^d - 1)) = 1$, this means that $a \equiv 0 \pmod{n_1}$. Since $(\delta\beta)^{n_1(q^l-1)} = 1$ we conclude that $\delta\beta$ is an element of order $n_1(q^l - 1)$.

Theorem 4.3. *Let* V_l^{*+} *be an irreducible cyclic* $(n_1(q^l - 1), m)$ *code over* $\mathrm{GF}(q^l)$ *with generator matrix*

$$G_l^{*+} = [1, \gamma, \gamma^2, \ldots, \gamma^{n-1}].$$

Let $d = \gcd(\mathrm{ord}_{n_1}(q), l)$.

If $\gcd(n_1,(q^l-1)/(q^d-1))=1$, *then there exists an element* δ *of* $GF(q^l)$, *and an element* β *of order* $n_1(q^d-1)$ *such that*

(i) $G_l^{*+}=[1,\delta\beta,\delta^2\beta^2,\ldots,\delta^{n_1(q^l-1)-1}\beta^{n_1(q^l-1)-1}]$

and

(ii) $G_d^{*+}=[1,\beta,\beta^2,\ldots,\beta^{n_1(q^d-1)-1}]$

is a generator matrix for an irreducible cyclic $(n_1(q^d-1),m)$ *code over* $GF(q^d)$.

Proof. By Lemma A.2 we have an irreducible cyclic $(n_1(q^d-1),m)$ code over $GF(q^d)$. Let β_0 be a root of the parity check polynomial of this code. By Theorem 4.2 we can choose δ_0 such that $\delta_0\beta_0$ is an element of order $n_1(q^l-1)$. Then $\delta_0\beta_0=\gamma^s$ for some s where $\gcd(s,n_1(q^l-1))=1$. Let $rs\equiv 1 \pmod{n_1(q^l-1)}$. Then $\delta=\delta_0^r$ and $\beta=\beta_0^r$ satisfy Theorem 4.3 since $\gcd(r,n_1(q^d-1))=1$.

Corollary 4.4. *Let* $A_l^*(z)$ *denote the weight enumerator polynomial of* V_l^*. *Under the conditions of Theorem* 4.3,

$$A_l^*(z)=\sum_{i=0}^{n_1}\sum_{j=0}^{m}A_{ij}(q^l-1)(q^l-q^d)\cdots(q^l-q^{d(j-1)})z^i$$

where A_{ij} *is the number of* $(m-j)$*-dimensional subspaces of* $GF(q^d)^m$ *which contain exactly* n_1-i *of the* n_1 *columns of* G_d^*.

Proof. By definition and by Theorem 4.3 we have

$$G_l^*=[1,\delta\beta,\delta^2\beta^2,\ldots,\delta^{n_1-1}\beta^{n_1-1}]$$

and

$$G_d^*=[1,\beta,\beta^2,\ldots,\beta^{n_1-1}].$$

Then the conditions of Theorem 3.2 hold and the corollary follows.

If $\gcd(n_1,(q^l-1)/(q^d-1))>1$, then by Theorem A.6 $\gcd(n_1,m)>1$. We then can express the weight enumerator polynomial $A_l^*(z)$ by the weight enumerator polynomial of $A_{l'}^*(z)$ for some d'.

Lemma 4.5. *Suppose* $e\mid\gcd(n_1,m)$ *and let* $n_1'=n_1/e$, $m'=m/e$. *Suppose* $\mathrm{ord}_{n_1'(q^l-1)}(q^l)=m'$ *and let* V_l^{*+} *denote an irreducible* $(n_1(q^l-1),m)$ *code over* $GF(q^l)$ *with check polynomial* $h(x)$. *Then there exists an irreducible* $(n_1'(q^l-1),m')$ *code,* $V_l^{*+'}$ *say, over* $GF(q^l)$ *with check polynomial* $h'(x)$ *for which*

(i) $h(x)=h'(x^e)$,

(ii) V_l^{*+} *is the direct sum of* e *copies of* $V_l^{*+'}$,

(iii) $A(z)=(A'(z))^e$.

Proof. We only prove (i) since (ii) and (iii) follow easily from (i). Let β be a primitive $n_1(q^l-1)$th root of unity in $GF(q^{ml})$. Then $\beta'=\beta^e$ is a primitive $n_1'(q^l-1)$ root of unity in $GF(q^{m'l})$. Suppose $h'(\beta')=0$. Then $h'(\beta')=0=h'(\beta^e)$,

which means that β is a root of $h'(x^e)$. Since $h(x)$ is irreducible and has the same degree as $h'(x^e)$, we get $h(x) = h'(x^e)$.

Theorem 4.6. *Let V_1^{*+} be an irreducible cyclic $(n_1(q^l-1), m)$ code over $\mathrm{GF}(q^l)$. Then V_1^{*+} is the direct sum of e copies of $V_1^{*+'}$, where $V_1^{*+'}$ is an irreducible cyclic $((n_1/e)(q^l-1), m/e)$ code over $\mathrm{GF}(q^l)$ with $\gcd(n_1/e, (q^l-1)/(q^{d'}-1)) = 1$ where $d' = \gcd(\mathrm{ord}_{n_1/e}(q), l)$.*

Proof. By Theorem A.6 there exists an $e \mid \gcd(n_1, m)$ such that $\gcd(n_1/e, (q^l-1)/(q^{d'}-1)) = 1$, where $d' = \gcd(\mathrm{ord}_{n_1/e}(q), l)$ and $\mathrm{ord}_{(n_1/e)(q^l-1)}(q^l) = m/e$. By Lemma 4.5 (ii) we get the desired result.

In the appendix we not only prove that there exists an e such that $\gcd(n_1/e, (q^l-1)/(q^{d'}-1)) = 1$, but we find the maximal e with this property. Using this result and the previous ones we get

Corollary 4.7. *Let V be an irreducible $(n_1(q^l-1), ml)$ code over $\mathrm{GF}(q)$, and let $A(z)$ be the weight enumerator polynomial of V. Then*

$$A(z) = \left(\sum_{i=0}^{n_1/e_0} \sum_{j=0}^{m/e_0} A_{ij} (q^l-1)(q^l-q^{d_0}) \cdots (q^l - q^{d_0(j-1)}) z^{q^{l-1}(q-1)i} \right)^{e_0}$$

where e_0 is defined in Theorem A.9, $d_0 = \gcd(\mathrm{ord}_{n_1/e_0}(q), l)$ and A_{ij} denotes the number of $((m/e_0)-j)$-dimensional subspaces of $\mathrm{GF}(q^{d_0})^{m/e_0}$ which contain exactly $((n_1/e_0)-i)$ of the n_1/e_0 column vectors of $G_{d_0}^*$ (the generator matrix of the $(n_1/e_0, m/e_0)$ code $V_{d_0}^* \subset \mathrm{GF}(q^{d_0})^{n_1/e_0}$).

Proof. This is an immediate consequence of Corollary 4.4, Lemma 4.5, Theorem 4.6, Theorem A.9, and Lemma 2.4.

Example. We want to find the weight enumerator polynomials of $(n, k) = (175(2^l-1), ml)$ irreducible cyclic codes over GF(2) which have $d = \gcd(\mathrm{ord}_{175}(2), l) = 3$. By Theorem A.2 $m = 140$ and by Theorem A.9 $e_0 = 35$ Therefore we get from Corollary 4.7 and Theorem 2.6

$$A(z) = \left(\sum_{i=0}^{5} \binom{5}{i} \frac{(2^l-1)^i + (2^l-1)(-1)^i}{2^l} z^{2^{l-1}i} \right)^{35}.$$

In the appendix we determine the n_1's for which we have $m/e_0 = (n_1/e_0) - 1$ and $m/e_0 = 2$ (Theorem A.11 and Theorem A.12). For those values of n_1 the weight enumerator polynomial may be found from Theorem 2.6, Theorem 2.7, and Corollary 4.7.

5. A generalisation

It is possible to extend the results obtained here and get $A(z)$ for irreducible cyclic codes with block lengths

$$n = n_1 \frac{q^l - 1}{N}$$

where $N \mid q-1$, $\gcd(n_1, N) = 1$, and $\gcd(l, N) = 1$. For these codes it is possible to find $A(z)$ in a similar way, but we can usually not find the complete weight enumerator polynomial since the nonzero elements no longer occur equally often when $N > 1$.

To show how the results extend we prove the following theorem.

Theorem 5.1. *Let V be an irreducible cyclic (n, k) code over $\mathrm{GF}(q)$, where $n = xy$ and $y \mid q-1$. If $N \mid y$ and $\gcd(N, x) = 1$, then there exists an irreducible cyclic $(n/N, k)$ code V' over $\mathrm{GF}(q)$ and*

$$A'(z) = A(z^{1/N})$$

where $A(z)$ and $A'(z)$ denote the weight enumerator polynomials of V and V' respectively.

Proof. Let β be an element in $\mathrm{GF}(q^k)$ of order $n = xy$. By Definition 1.1

$$V = \{v(c) \mid v(c) = (\mathrm{Tr}_1^k(c), \mathrm{Tr}_1^k(c\beta), \ldots, \mathrm{Tr}_1^k(c\beta^{n-1}), c \in \mathrm{GF}(q^k)\}.$$

Put

$$V' = \{v(c) \mid v(c) = \mathrm{Tr}_1^k(c), \mathrm{Tr}_1^k(c\beta^N), \ldots, \mathrm{Tr}_1^k(c\beta^{N(n/N-1)}), c \in \mathrm{GF}(q^k)\}.$$

To show that V' is an irreducible cyclic $(n/N, k)$ code over $\mathrm{GF}(q)$, it is sufficient to show that $k = \mathrm{ord}_{n/N}(q)$. Let $k' = \mathrm{ord}_{n/N}(q)$. Then $k' \mid k$. Let $y_1 = \prod_{p \mid N} p^{v_p(y)}$ and let $y = y_1 y_2$. Then $\gcd(y_1, y_2 x) = 1$. Since $xy_2 \mid n/N \mid q^{k'} - 1$ and $y_1 \mid y \mid q-1 \mid q^{k'} - 1$ we have that $xy_1y_2 = n \mid q^{k'} - 1$. Hence $k \mid k'$ and therefore $k = k'$.

Put $j = j_2 x + j_1$, $0 \leq j_1 < x$, $0 \leq j_2 < y$, and put $t = t_2 x + t_1$, $0 \leq t_1 < x$, $0 \leq t_2 < y/N$. If we let $v(c) = (v_0(c), v_1(c), \ldots, v_{n-1}(c)) \in V$ and $v'(c) = (v_0(c), v_1(c), \ldots, v_{n/N-1}(c)) \in V'$, then we can write

$$v_j(c) = \beta^{j_2 x} \mathrm{Tr}_1^k(c\beta^{j_1})$$

and

$$v'_t(c) = \beta^{t_2 N x} \mathrm{Tr}_1^k(c\beta^{Nt_1}).$$

We also have that $\mathrm{Tr}_1^k(c\beta^j) = 0$ if and only if $\mathrm{Tr}_1^k(c\beta^{j_0}) = 0$ where $j \equiv j_0 \pmod{x}$ and $0 \leq j_0 < x$. Since $\gcd(N, x) = 1$, Nt_1 runs through a complete residue system (mod x) when t_1 does. Let $A^*(z)$ denote the weight enumerator polynomial of the linear code

$$V^* = \{v^*(c) \mid v^*(c) = (\mathrm{Tr}_1^k(c), \mathrm{Tr}_1^k(c\beta), \ldots, \mathrm{Tr}_1^k(c\beta^{x-1}), c \in \mathrm{GF}(q^k)\}.$$

Then we have

$$A'(z) = A^*(z^{\gamma/N})$$

and

$$A(z) = A^*(z^{\gamma}).$$

Hence $A'(z) = A(z^{1/N})$ which was to be proved.

We now let V be an irreducible cyclic code with block length $n = n_1(q^l - 1)$. Let $N \mid q-1$, $\gcd(n_1, N) = 1$, and $\gcd(l, N) = 1$. We write $n = n_1((q^l-1)/(q-1))(q-1)$ and put $x = n_1((q^l-1)/(q-1))$ and $y = q-1$. Then $N \mid y$ and $\gcd(N, x) = 1$, since $\gcd(n_1((q^l-1)/(q-1)), N) = \gcd(n_1 l, N) = 1$. By Theorem 5.1 there exists an irreducible cyclic code V' with block length $n = n_1((q^l-1)/N)$ which has the same dimension as V and with $A'(z) = A(z^{1/N})$. We can therefore find the weight enumerator polynomials of all irreducible cyclic codes of block lengths $n = n_1((q^l-1)/N)$ with $N \mid q-1$, $\gcd(n_1, N) = 1$, and $\gcd(l, N) = 1$, by finding $A(z)$ for irreducible cyclic codes with block length $n = n_1(q^l - 1)$ and put $A'(z) = A(z^{1/N})$.

6. Bounds on the region in the (i, j)-plane where $A_{ij} > 0$

If we let the integers A_{ij} be arranged in an $n_1 \times m$ array, then we are going to prove that certain elements in the upper right and the lower left corners have to be 0.

Throughout the section we will assume that the sequence of codes for which we compute the integers A_{ij}, is the sequence V_l^* defined in Section 2. (Though, it is not hard to see that Theorem 2.1 applies to the more general situation adopted in Section 3).

The codes in the sequence V_l^* are irreducible only when $\gcd(l, r) = d$ for some fixed d, and the generator matrix G_d for V_d^* is over $GF(q^d)$. In Sections 6, 7, and 8 we will assume $d = 1$. This is no restriction, since we may suppose that q^d has been replaced by q beforehand.

We will identify $GF(q^m)$ and $GF(q)^m$. This is possible since each element in $GF(q^m)$ may be represented by an m-dimensional vector over $GF(q)$. Thus we sometimes write $\mathrm{Tr}_1^m(u)$ where $u \in GF(q)^m$, instead of $\mathrm{Tr}_1^m(a_u)$ where a_u is the element in $GF(q^m)$ which is represented by u.

Theorem 6.1. *For $j = 0, 1, 2, \ldots, m$, let*

$$B_j = \min\{i \mid A_{ij} > 0\}$$

and

$$C_j = \max\{i \mid A_{ij} > 0\}.$$

Then

$$0 = B_0 < B_1 < \cdots < B_m = n_1$$

and

$$0 = C_0 < C_1 < \cdots < C_k = C_{k+1} = \cdots = C_m = n_1$$

for some $k \geq 1$.

Example. Let V_1^* be the irreducible (9, 6) code over GF(2). The array (A_{ij}) is given below

i \ j	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	9	0	0	0	0	0
3	0	0	3	0	0	0	0
4	0	27	27	0	0	0	0
5	0	0	54	18	0	0	0
6	0	27	126	54	3	0	0
7	0	0	243	270	27	0	0
8	0	0	162	621	216	9	0
9	0	0	36	432	605	54	1

Thus

$$(B_0, B_1, B_2, B_3, B_4, B_5, B_6) = (0, 2, 3, 5, 6, 8, 9),$$

$$(C_0, C_1, C_2, C_3, C_4, C_5, C_6) = (0, 6, 9, 9, 9, 9, 9).$$

Proof. Let $G_1 = [1, \beta, \beta^2, \ldots, \beta^{n_1-1}]$ be the generator matrix for V_1^*. Let S denote the set of column vectors of G_1, and let $U_j^{(1)}, U_j^{(2)}, \ldots, U_j^{(T_j)}$ denote the distinct j-dimensional subspaces of $\mathrm{GF}(q)^m$. All the vectors in S are distinct since β is a primitive nth root of unity and $n_1 \leq n$. From Theorem 3.2 we get

$$A_{i,m-j} = |\{t \mid |U_j^{(t)} \cap S| = n_1 - i\}| = |\{t \mid i = n_1 - |U_j^{(t)} \cap S|\}|.$$

Therefore

$$B_{m-j} = \min(i \mid A_{i,m-j} > 0) = \min_t (n_1 - |U_j^{(t)} \cap S|) = n_1 - \max_t |U_j^{(t)} \cap S|,$$

$$C_{m-j} = \max(i \mid A_{i,m-j} > 0) = \max_t (n_1 - |U_j^{(t)} \cap S|) = n_1 - \min_t |U_j^{(t)} \cap S|. \tag{6.1}$$

We assume $0 \leq j < m$ and choose a t_0 for which

$$B_{m-j} = n_1 - |U_j^{(t_0)} \cap S|.$$

Let $v \in S - U_j^{(t_0)}$. Such a v exists because $j < m$ and S contains m linearly independent vectors. We put

$$U_{j+1}^{(t_0)} = \{u + cv \mid u \in U_j^{(t_0)}, c \in \mathrm{GF}(q)\}.$$

Obviously

$$U_{j+1}^{(t_1)} \cap S \supset (U_j^{(t_0)} \cap S) \cup \{v\}.$$

Therefore

$$B_{m-(j+1)} = n_1 - \max_t |U_{j+1}^{(t)} \cap S| \leq n_1 - |U_{j+1}^{(t_1)} \cap S| \leq n_1 - |U_j^{(t_0)} \cap S| - 1 = B_{m-j} - 1.$$

So we have proved that $B_j < B_{j+1}$. Since $|GF(q)^m \cap S| = |S| = n_1$, and since $|\{0\} \cap S| = 0$, we have that $B_0 = 0$ and $B_m = n_1$, and we have proved the assertion in Theorem 6.1 concerning the B_j's.

Let r' be the least integer for which $|U_{r'+1}^{(t)} \cap S| > 0$ for all t. If $0 \leq j \leq r'$ we have that there exists a t_2 for which $|U_j^{(t_2)} \cap S| = 0$. From (6.1) we conclude that $C_{m-j} = n_1$ for $0 \leq j \leq r'$, or that $C_j = n_1$, for $r = m - r' \leq j \leq m$.

We now assume $r' < j$, and choose a t_3 for which

$$C_{m-j} = n_1 - |U_j^{(t_3)} \cap S|.$$

Let $u_1, u_2, \ldots, u_j$ be a basis for $U_j^{(t_3)}$, and assume that $u_j \in S$. Such a basis exists because $r' < j$ and therefore $|U_j^{(t_3)} \cap S| > 0$. Let $U_{j-1}^{(t_4)}$ be the vector space spanned by $u_1, u_2, \ldots, u_{j-1}$. Then $u_j \in U_j^{(t_3)} \cap S$ but $u_j \notin U_{j-1}^{(t_4)} \cap S$. Thus

$$C_{m-(j-1)} = n_1 - \min_t (U_{j-1}^{(t)} \cap S) \geq n_1 - |U_{j-1}^{(t_4)} \cap S|$$

$$\geq n_1 - |U_j^{(t_3)} \cap S| + 1 = C_{m-j} + 1 > C_{m-j}$$

which proves that $C_j < C_{j+1}$ for $0 \leq j < r$, and Theorem 6.1 is proved.

7. Symmetries in the semiprimitive case

In this section we derive a symmetry in the integers A_{ij} when V_1^* is semiprimitive. This symmetry was first observed from the numerical results (See Tables 6 and 7).

Let G_1 be an arbitrary but fixed generator matrix for V_1^*. Then all column vectors in G_1 are distinct. This is true if we choose $G_1 = [1, \beta, \beta^2, \ldots, \beta^{n_1-1}]$. Therefore it must be true for any generator matrix G_1 for V_1^*.

From this and from Lemma 3.1 it follows that the weight of a code word corresponding to a vector $x \in K_U$ is given by

$$w(G_1, U) = n_1 - |S \cap U| = n_1 - z. \tag{7.1}$$

If $U_\perp$ denotes the dual vector space of U we have that

$$z = |S \cap U| = |\{s \in S \mid s \cdot u_\perp = 0, \forall u_\perp \in U_\perp\}|. \tag{7.2}$$

We consider the subcode $\tau(U_\perp)$ of V_1^* defined by

$$\tau(U_\perp) = \{u_\perp \cdot G_1 \mid u_\perp \in U_\perp\}. \tag{7.3}$$

Thus τ is a one to one mapping from the family of subspaces of $GF(q)^m$ onto the family of subcodes of V_1^*.

Suppose that $\dim(U_\perp) = j$, and that we have numbered the code words in $\tau(U_\perp)$ from 0 to $q^j - 1$. Let $\boldsymbol{D}$ denote the $q^j \times n_1$-matrix, whose ith row is the ith code word in $\tau(U_\perp)$.

Since the rows of $\boldsymbol{D}$ constitute a vector space of dimension j over GF(q), a column in $\boldsymbol{D}$ either contains zeroes only, or each element from GF(q) occurs exactly q^{j-1} times in it. In the latter case the column contains $(q-1)q^{j-1}$ nonzero elements. From (7.2) we see that the number of columns which contain only zeroes is z. By counting the nonzero elements in $\boldsymbol{D}$ in two different ways we obtain,

$$(n_1 - z)q^{j-1}(q-1) = \sum_{i=1}^{q^j-1} w_i. \tag{7.4}$$

Here w_i is the Hamming weight of the ith code word in $\tau(U_\perp)$. (We let $w_0 = 0$ be the weight of the allzero code word). Using (7.1)–(7.4) we obtain

Lemma 7.1. *Let w_i, $i = 0, 1, 2, \ldots, q^j - 1$, be the Hamming weight of the ith code word in the subcode $\tau(U_\perp)$ of V_1^*. Then*

$$w(G_1, U) = \frac{1}{q^{j-1}(q-1)} \sum_{i=0}^{q^j-1} w_i,$$

where $j = \dim(U_\perp) = m - \dim(U)$.

An irreducible (n, k) code is said to be semiprimitive if k is even and there exists a divisor k' of $k/2$ for which $(q^k - 1)/n \mid q^{k'} + 1$. It is shown in [1] that in this case one nonzero cycle (that is n code words), has Hamming weight W_0', say, and all the other nonzero cycles have the same weight, which we denote by W_1'.

If V_1^{*+} is semiprimitive, then V_1^* contains $n_1(q-1)$ code words of weight $W_0 = W_0'/(q-1)$ and $q^m - 1 - n_1(q-1)$ code words of weight $W_1 = W_1'/(q-1)$.

Theorem 7.2. *If V_1^{*+} is semiprimitive, then the corresponding integers A_{ij} satisfy,*

$$A_{ij} = A_{i'j'}$$

where

$$i' = q^{1+j-m}\left((n_1 - i)W_0 + \left(\frac{q^{m-j}-1}{q-1} - n_1 + i\right)W_1\right)$$

and

$$j' = m - j.$$

Proof. Let ψ be a primitive root in $GF(q^m)$, and put $\beta = \psi^{(q^m-1)/n}$. We choose a t_0 for which

$$(\mathrm{Tr}_1^m(\psi^{t_0}), \mathrm{Tr}_1^m(\psi^{t_0}\beta), \ldots, \mathrm{Tr}_1^m(\psi^{t_0}\beta^{n_1-1}))$$

is a code word in V_1^* of weight W_0. (According to [1] we may choose $t_0 = 0$ unless

$N = (q^k - 1)/n$ is even and $(q^{k'} + 1)/N$ is odd, in which case we may choose $t_0 = N/2$). We now choose as a generator matrix for V_1^*,

$$G_1 = [\psi^{t_0}, \psi^{t_0}\beta, \ldots, \psi^{t_0}\beta^{n_1-1}].$$

This is a generator matrix because β is a root of an irreducible polynomial of degree m over GF(q), and so any m consecutive columns will be linearly independent over GF(q). Therefore the m rows are linearly independent.

We also note that no two distinct columns in G_1 are multiples of each other. For if $c\psi^{t_2}\beta^{t_1} = \psi^{t_2}\beta^{t_1+t_2}$, with $0 < t_2 < n_1$ and $c \in \mathrm{GF}(q)$, then $c = \beta^{t_2} \in \mathrm{GF}(q)$, and so $\beta^{t_2(q-1)} = 1$. But this is impossible since β is a primitive $n_1(q-1)^{\text{th}}$ root of unity and $t_2 < n_1$.

Let A be defined by

$$A = |\{U' \mid \dim U' = m - j, |U' \cap S| = n_1 - i\}|.$$

From (7.1) and the definition of A_{ij} it follows that $A_{ij} = A$. We now define a mapping φ, from the family of subspaces of $\mathrm{GF}(q)^m$ onto the family of subcodes of V_1^* as follows

$$\varphi(u') = \{c_{u'} \mid c_{u'} = (\mathrm{Tr}_1^m(u'), \mathrm{Tr}_1^m(u'\beta), \ldots, \mathrm{Tr}_1^m(u'\beta^{n_1-1})), u' \in U'\},$$

and put $\tau(U_\perp) = \varphi(U')$ or $U_\perp = \tau^{-1}\varphi(U')$ (see (7.3)).

From the definition of t_0 it follows that $w(c_{u'}) = W_0$ if and only if $u' = \psi^{t_0}\beta^t$ for some t, $0 \leq t < n$. That is, if and only if $u' = cs$ for some $s \in S$ and $c \in \mathrm{GF}(q)$ (Lemma 2.3). Since S does not contain two vectors which are multiples of each other, $\tau(U_\perp) = \varphi(U')$ contains $(q-1)|U' \cap S| = (q-1)(n_1 - i)$ code words of weight W_0, and $q^{m-j} - 1 - (q-1)(n_1 - i)$ code words of weight W_1. Using Lemma 7.1 we obtain

$$w(G_1, U) = \frac{1}{q^{m-j-1}(q-1)}((q-1)(n_1-i)W_0 + (q^{m-j} - 1 - (q-1)(n_1-i))W_1)$$

$$= q^{1+j-m}\left((n_1-i)W_0 + \left(\frac{q^{m-j}-1}{q-1} - n_1 + i\right)W_1\right).$$

The relation $U_\perp = \tau^{-1}\varphi(U')$ establishes a one-to-one correspondence between the subspaces U' of dimension $m - j$ and the subspaces U of dimension j. Therefore $A = A_{ij}$, and Theorem 7.2 is proved.

8. Formulae for A_{ij} when $m - j$ is small

Our next theorem gives A_{ij} when $m - j$ is small. In particular when V_1^* is a maximum distance separable (MDS) code, we will determine every A_{ij}.

To simplify the notations we define

$$\begin{bmatrix} m \\ j \end{bmatrix} = \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{j-1})}{(q^j-1)(q^j-q)\cdots(q^j-q^{j-1})} \quad \text{when } j \geq 1,$$

$$= 1 \quad \text{when } j = 0.$$

Note that $\begin{bmatrix} m \\ j \end{bmatrix}$ is the number of j-dimensional subspaces of $GF(q)^m$.

Theorem 8.1. *Let i_0 be the largest integer such that any i_0 vectors from S will be linearly independent.*

If $m - j < i_0$, then

$$A_{ij} = \binom{n_1}{i} \sum_{h=0}^{m+i-j-n_1} (-1)^h \binom{i}{h} \begin{bmatrix} m-n_1+i-h \\ j \end{bmatrix}.$$

Proof. Let $S_1 \subset S$, $|S_1| = i$, and let $i \leq j < i_0$. We define $B_j(S_1)$ by

$$B_j(S_1) = |\{U \mid U \subset GF(q^m), U \text{ vectorspace, dim } U = j, U \cap S = S_1\}|$$

and $D_j(S_1)$ by

$$D_j(S_1) = |\{U \mid U \subset GF(q^m), U \text{ vectorspace, dim } U = j, U \supset S_1\}|.$$

We then have that

$$\sum_{S_1 \subset S_2 \subset S} B_j(S_2) = D_j(S_1). \tag{8.1}$$

We have that $D_j(S_1)$ equals the number of j-dimensional subspaces of $GF(q^m)$ which contain the fixed i-dimensional subspace U_1 spanned by S_1. Therefore $D_j(S_1)$ is equal to the number of $(j-i)$-dimensional subspaces of $GF(q^m)/U_1$, and so

$$D_j(S_1) = \begin{bmatrix} m-i \\ j-i \end{bmatrix}.$$

We then get from (8.1) that

$$\sum_{S_1 \subset S_2 \subset S} B_j(S_2) = \begin{bmatrix} m-i \\ j-i \end{bmatrix}. \tag{8.2}$$

We next show that $B_j(S_1)$ does only depend on $|S_1| = i$ when $j < i_0$. If $j - i = 0$, then $B_j(S_1) = 1$. Therefore $B_i(S_1)$ does not depend on S_1. Suppose we have proved that $B_j(S_1)$ does not depend on S_1 for $j - i < t$ and $j < i_0$. We get from (8.2)

$$B_j(S_1) + \sum_{\substack{S_1 \subset S_2 \subset S \\ S_1 \neq S_2}} B_j(S_2) = \begin{bmatrix} m-i \\ j-i \end{bmatrix}.$$

If $j - i = t$ and $j < i_0$, then by the induction hypotheses the terms under the summation sign do not depend on S_2 since $|S_2| > i$. Therefore $B_j(S_1)$ does not depend on S_1. We may therefore put $B_j(S_1) = B_{ij}$.

Using this we rewrite (8.2) as follows:

$$\sum_{i_2=i}^{j} \binom{n_1-i}{i_2-i} B_{i_2,j} = \sum_{h=0}^{j-i} \binom{n_1-i}{h} B_{i+h,j} = \begin{bmatrix} m-i \\ j-i \end{bmatrix}.$$

By [12, p. 49] this is equivalent to

$$B_{ij} = \sum_{h=0}^{j-i} (-1)^h \binom{n_1-i}{h} \begin{bmatrix} m-i-h \\ m+j \end{bmatrix}.$$

By the definitions of B_{ij} and A_{ij} we have that

$$A_{ij} = \binom{n_1}{i} B_{n_1-i,m-j} = \binom{n_1}{i} \sum_{h=0}^{m-n_1+i-j} (-1)^h \binom{i}{h} \begin{bmatrix} m-n_1+i-h \\ j \end{bmatrix},$$

and Theorem 8.1 is proved.

An (n, k) code is defined to be MDS if and only if the minimal weight of a nonzero code word is $n-k+1$.

We have that V_1^* is MDS if and only if $V_1^\perp$ is MDS, because these two codes have the same dimension and minimal weight. The weight enumerator for an MDS code is known, see [11]. Using this we get the following theorem.

Theorem 8.2. *Let V_1^* be an MDS code over GF(q). Then the weight enumerator polynomial $A_1^*(z)$ for V_1^* is given by*

$$A_1^*(z) = 1 + \sum_{i=0}^{n_1} z^i \binom{n_1}{i} \sum_{h=0}^{i-1-(n_1-m)} (-1)^h \binom{i}{h} (q^{i(i-h-(n_1-m))} - 1).$$

Above we derived Theorem 8.2 from the known weight enumerator for MDS codes. But when V_1^* is MDS, then $i_0 = m$ in Theorem 4.1, since the dual code $V_1^{*\perp}$ is also MDS by [11], and we can determine $A_1^*(z)$ completely. We now derive Theorem 8.2 from Theorem 8.1.

By Theorem 3.2 and by Theorem 8.1 we get that $A_1^*(z)$ is equal to

$$1 + \sum_{i=1}^{n_1} z^i \sum_{j=1}^{m} A_{ij} (q^i - 1)(q^i - q) \cdots (q^i - q^{i-1})$$

$$= 1 + \sum_{i=1}^{n_1} z^i \binom{n_1}{i} \sum_{j=1}^{m} (q^i - 1)(q^i - q) \cdots (q^i - q^{i-1}) \sum_{h=0}^{m+i-j-n_1} (-1)^h \binom{i}{h} \times \begin{bmatrix} m-n_1+i-h \\ j \end{bmatrix}.$$

We define $\begin{bmatrix} r \\ s \end{bmatrix} = 0$ when $r < s$. Then we get that $A_1^*(z)$ is

$$1 + \sum_{i=1}^{n_1} z^i \binom{n_1}{i} \sum_{j=1}^{\infty} (q^i - 1)(q^i - q) \cdots (q^i - q^{i-1}) \sum_{h=0}^{\infty} (-1)^h \binom{i}{h} \begin{bmatrix} m-n_1+i-h \\ j \end{bmatrix}$$

$$= 1 + \sum_{i=1}^{n_1} z^i \binom{n_1}{i} \sum_{h=0}^{\infty} (-1)^h \binom{i}{h} \sum_{j=1}^{\infty} \begin{bmatrix} m-n_1+i-h \\ j \end{bmatrix} (q^i - 1) \times (q^i - q) \cdots (q^i - q^{i-1}).$$

According to [9, p. 76] we have that

$$x^n - 1 = \sum_{j=1}^{n} \begin{bmatrix} n \\ j \end{bmatrix} (x-1)(x-q)\cdots(x-q^{j-1}).$$

If we let $x = q^l$, then we get

$$\sum_{j=1}^{\infty} \begin{bmatrix} n \\ j \end{bmatrix} (q^l-1)(q^l-q)\cdots(q^l-q^{j-1}) = q^{ln} - 1 \quad \text{when } n > 0,$$

$$= 0 \quad \text{when } n \leq 0.$$

Hence

$$A_i^*(z) = 1 + \sum_{i=1}^{n_1} z^i \binom{n_1}{i} \sum_{h=l_i}^{m-n_1+i-1} (-1)^h \binom{i}{h} (q^{l(m-n_1+i-h)} - 1).$$

9. The weight enumerator polynomials for some irreducible cyclic codes with block lengths $n = ((q^f-1)/(q^d-1)) \cdot ((q^l-1)/n)$

In this section we will find the weight enumerator polynomials of all irreducible cyclic codes with block lengths

$$n = n_1 \frac{q^l - 1}{N}$$

with

$$n_1 = \frac{q^f - 1}{q^d - 1},$$

$d = \gcd(\mathrm{ord}_{n_1}(q), l)$, $N \mid q-1$, $\gcd(n_1, N) = 1$, and $\gcd(l, N) = 1$. The codes considered here have f/d nonzero weights. In particular when $f = d$, we get a class of equidistant codes whose weight distributions are well known [10]. Note that we have $r = f$.

Theorem 9.1. *Let V be an irreducible cyclic (n, ml) code with block length $n = n_1((q^l-1)/N)$.*

If $n_1 = (q^f-1)/(q^d-1)$, $d = \gcd(\mathrm{ord}_{n_1}(q), l)$, $N \mid q-1$, $\gcd(n_1, N) = 1$, and $\gcd(l, N) = 1$, then $m = f/d$ and

$$A(z) = \sum_{j=0}^{m} \prod_{i=0}^{j-1} \frac{q^f - q^{di}}{q^{dj} - q^{di}} \prod_{a=0}^{j-1} (q^l - q^{da}) z^{((q^f-q^{f-dj})/(q^d-1))q^{l-1}(q-1/N)}.$$

Proof. By Theorem 5.1 it is sufficient to prove the theorem for $N = 1$.

By definition and by Lemma A.2 we have

$$m = \mathrm{ord}_{n_1(q^d-1)}(q^d) = \mathrm{ord}_{q^r-1}(q^d) = \frac{r}{d}.$$

We now find $A(z)$. Since $\gcd(n_1, (q^l-1)/(q^d-1)) = 1$ we can apply Theorem 4.3 which gives that V_d^{*+} is an irreducible cyclic $(n_1(q^d-1), m)$ code over $\mathrm{GF}(q^d)$.

Since $n_1 = (q^r - 1)/(q^d - 1)$ and $m = r/d$, V_d^* is an $(q^r - 1, r/d)$ maximal shift register code over $\mathrm{GF}(q^d)$. By Theorem 4.3

$$G_d^* = [1, \beta, \ldots, \beta^{n_1 - 1}]$$

where $\beta^{n_1(q^d-1)} = 1$. Suppose

$$\beta^i = a\beta^j$$

where $a \in \mathrm{GF}(q^d)$ and $0 \leq i \leq j < n_1$. Then

$$\beta^{(j-i)(q^d-1)} = 1$$

which means that $n_1 \mid j - i$. Hence $i = j$. Therefore G_d^* contains $(q^r - 1)/(q^d - 1)$ nonzero columns which are not multiples over $\mathrm{GF}(q^d)$. If $A_l^*(z)$ denotes the weight enumerator polynomial of V_l^*, then we get from Corollary 4.4

$$A_l^*(z) = \sum_{i=0}^{n_1} \sum_{j=0}^{m} A_{ij} \prod_{a=0}^{j-1} (q^l - q^{da}) z^l$$

where A_{ij} is the number of $(m-j)$-dimensional subspaces of $\mathrm{GF}(q^d)^m$ which contains exactly $n_1 - i$ of the n_1 columns of G_d^*. Let W denote a subspace of $\mathrm{GF}(q^d)^m$ of dimension $m - j$. Then W contains exactly $(q^{r-dj} - 1)/(q^d - 1)$ of the n_1 columns of G_d^*. Therefore we get

$$A_{ij} = \prod_{b=0}^{m-j-1} \frac{q^r - q^{db}}{q^{r-dj} - q^{db}} \quad \text{if } n_1 - i = \frac{q^{r-dj} - 1}{q^d - 1}.$$

$$= 0 \qquad \text{if } n_1 - i \neq \frac{q^{r-dj} - 1}{q^d - 1},$$

which is the same as

$$A_{ij} = \prod_{b=0}^{j-1} \frac{q^r - q^{db}}{q^{dj} - q^{db}} \quad \text{if } i = \frac{q^r - q^{r-dj}}{q^d - 1},$$

$$= 0 \qquad \text{if } i \neq \frac{q^r - q^{r-dj}}{q^d - 1}.$$

Hence

$$A_l^*(z) = \sum_{j=0}^{m} \prod_{b=0}^{j-1} \frac{q^r - q^{db}}{q^{dj} - q^{db}} \prod_{a=0}^{j-1} (q^l - q^{da}) z^{(q^r - q^{r-dj})/(q^d-1)}.$$

From Lemma 2.4 and Theorem 5.1 we get the result.

Example. Let V be an irreducible cyclic $(21, 6)$ binary code. Then $n = 3(2^3 - 1)$ and we can apply Theorem 9.1 with $q = 2$, $r = \mathrm{ord}_3(2) = 2$, $l = 3$, $d = 1$, $N = 1$, and $m = 2$. We get

$$A(z) = \sum_{j=0}^{2} \prod_{i=0}^{j-1} \frac{2^2-2^i}{2^j-2^i} \prod_{a=0}^{j-1} (2^3-2^a)\, z^{((2^2-2^{2-j})/(2-1))2^{3-1}}$$

$$= 1 \cdot z^0 + \frac{2^2-1}{2-1}(2^3-1)\, z^{(2^2-2)4} + (2^3-1)(2^3-2)\, z^{(2^2-1)4}$$

$$= 1 + 21z^8 + 42z^{12}.$$

This agrees with Table 16.1 in Berlekamp [3].

Remark. Putting $d = f$ in Theorem 9.1 we get that an irreducible cyclic $((q^l-1)/N, l)$ code has

$$A(z) = 1 + (q^l-1)z^{q^{l-1}((q-1)/N)},$$

whenever $N \mid q-1$, $\gcd(l, N) = 1$. This was first proved by Oganesyan, Yagdzyan, and Tairyan [10].

10. Codes with small values of n_1

In this section we give a survey of the binary codes with $n_1 \leq 35$. In particular we give the complete weight enumerator polynomial of all binary codes with $n_1 \leq 17$.

Each entry in Table 1 gives the value of m. If the corresponding values of A_{ij} may be found from some general theorem this is indicated by a letter as follows:

A. Theorem 2.5 $(m = n_1)$.
B. Theorem 2.6 $(m = n_1 - 1)$.
C. Theorem 2.7 $(m = 2)$.
D. Theorem 9.1 $(n_1 = (2^{dm}-1)/(2^d-1))$.
E. Theorem 4.6 (direct sum of codes with lower parameters).
F. Theorem 8.2 (MDS code).

For some of the codes not covered by any general theorem, we have computed the values of A_{ij}. We developed an algorithm for enumerating the subspaces of a finite dimensional vector space over a finite field (this may appear in print later). Combining this with the definition of A_{ij} we wrote a FORTRAN program to compute the A_{ij} and we have run it on the UNIVAC 1110 at the University of Bergen for a number of values of n_1 and d. Some of these are given below. In particular we give complete information for all codes with $n_1 \leq 17$. In the tables, A_{ij} is found in row i and column j, with rows and columns numbered $0, 1, 2, \ldots$. In Table 8 we give the actual weight for the codes with $n_1 \leq 7$; to simplify the expressions we have put $2^l - 1 = L$.

Table 1.

n_1	d / r	1	2	3	4	5	6	7	8	9	10	11	12	14	18	20	28
3	2	2BD	3A														
5	4	4B	2C		5A												
7	3	3D		7A													
9	6	6E	9A	2C			9A										
11	10	10B	5			2C					11A						
13	12	12B	6	4	3F		2C						13A				
15	4	4D	6E		15A												
17	8	8	4		2C				17A								
19	18	18B	9	6			3			2C					19A		
21	6	6	3D	14E			21A										
23	11	11										23A					
25	20	20E	10E		25A	4					2C					25A	
27	18	18E	27A	6E			27A			2C					27A		
29	28	28B	14		7			4						2C			29A
31	5	5D				31A											
33	10	10	15E			2C					33A						
35	12	12	6	28E	15E		14E						35A				

Table 2. $n_1 = 11$, $d = 2$, $m = 5$.

1	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	55	0	0	0	0
0	55	0	0	0	0
0	55	165	0	0	0
0	110	660	55	0	0
0	55	2112	825	11	0
0	11	2860	4917	330	1

Table 3. $n_1 = 13$, $d = 2$, $m = 6$.

1	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	52	0	0	0	0	0
0	0	0	0	0	0	0
0	351	39	0	0	0	0
0	0	520	0	0	0	0
0	676	3536	286	0	0	0
0	0	13728	5772	78	0	0
0	286	35022	62959	4277	13	0
0	0	40248	307788	88738	1352	1

Table 4. $n_1 = 13$, $d = 3$, $m = 4$.

1	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	52	0	0	0
0	78	0	0	0
0	156	78	0	0
0	195	793	13	0
0	104	3874	572	1

Table 5. $n_1 = 17$, $d = 1$, $m = 8$.

1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	68	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	85	0	0	0	0	0	0	0
0	0	272	0	0	0	0	0	0
0	68	884	0	0	0	0	0	0
0	0	1428	476	0	0	0	0	0
0	34	1904	3808	34	0	0	0	0
0	0	2380	9520	2210	0	0	0	0
0	0	2108	19720	11900	680	0	0	0
0	0	1292	28220	39236	6528	136	0	0
0	0	459	25211	77605	30243	1887	17	0
0	0	68	10200	69802	59704	8772	238	1

Table 6. $n_1 = 17$, $d = 2$, $m = 4$.

1	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	68	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	136	0	0
0	17	85	17	0
0	0	136	68	1

Appendix

In this appendix we give some results whose proofs require some number theory. We give necessary and sufficient conditions for $k/l = n_1$ and for $k/l = n_1 - 1$ (Theorem A.3 below) in which cases the weight distributions are given by Theorems 2.5 and 2.6. Further we show the existence of an e satisfying the

requirements of Lemma 4.5, (Theorem A.6 below). Finally we find an explicit formula for the largest such e (Theorem A.9 below), a very useful result for the actual calculation of weight distribution polynomials.

Throughout the appendix a, n_1, and l are positive integers such that $a > 1$ and $\gcd(a, n_1) = 1$, p denotes a prime, $v_p(b)$ the (additive) p-adic valuation of b, and $\mathrm{ord}_b(c)$ the multiplicative order of c modulo b. Further

$$r = \mathrm{ord}_{n_1}(a), \quad d = \gcd(r, l),$$

$$m = \mathrm{ord}_{n_1(a^l-1)}(a^l),$$

$$s = \prod_{p \mid a^d-1} p^{v_p(n_1)}, \quad t = n_1/s,$$

$$u = \mathrm{ord}_t(a^d),$$

$$h = 1 \quad \text{if } s \text{ is odd or } a^d \equiv 1 \pmod 4,$$

$$= 2^{\min(v_2(s),\, v_2(a^d+1))-1} \quad \text{otherwise.}$$

The following well known facts (Lemma A.1) will be used repeatedly.

Lemma A.1. *Let $p \mid a - 1$. Then we have*

(i) $v_p(a^\mu - 1) = v_p(a+1) + v_p(\mu)$ *if* $p = 2$, $a \equiv 3 \pmod 4$, *and* μ *is even,*
$= v_p(a-1) + v_p(\mu)$ *otherwise.*

(ii) *If* $\gcd(b, c) = 1$, *then* $\mathrm{ord}_{bc}(a) = \mathrm{lcm}(\mathrm{ord}_b(a), \mathrm{ord}_c(a))$.

Table 7. $n_1 = 21$, $d = 1$, $m = 6$.

1	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	21	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	42	28	0	0	0	0
0	0	0	0	0	0	0
0	0	126	3	0	0	0
0	0	0	0	0	0	0
0	0	315	63	0	0	0
0	0	0	168	0	0	0
0	0	182	315	28	0	0
0	0	0	504	126	0	0
0	0	0	294	315	21	0
0	0	0	48	182	42	1

Table 8. Weights $= c \cdot 2^{l-1}$.

n	k	l	c 0	1	2	3	4	5	6	7
$3L$	$2l$	$(l,2)=1$	1	0	$3L$	L^2-L				
$3L$	$3l$	$(l,2)=2$	1	$3L$	$3L^2$	L^3				
$5L$	$4l$	$(l,4)=1$	1	0	$10L$	$10L^2-10L$	$5L^3-5L^2+5L$	$L^4-L^3+L^2-L$		
$5L$	$2l$	$(l,4)=2$	1	0	0	0	$5L$	L^2-3L		
$5L$	$5l$	$(l,4)=4$	1	$5l$	$10L^2$	$10L^3$	$5L^4$	L^5		
$7L$	$3l$	$(l,3)=1$	1	0	0	0	$7L$	0	$7L^2-7L$	L^3-4L^2+3L
$7L$	$7l$	$(l,3)=3$	1	$7L$	$21L^2$	$35L^3$	$35L^4$	$21L^5$	$7L^6$	L^7

Lemma A.2. *We have*

$$m = \mathrm{ord}_{n_1(a^d-1)}(a^d) = \mathrm{lcm}(sh^{-1}, u).$$

Proof. If $(r/d) \mid M$, then

$$\sum_{j=0}^{M-1} a^{jl} \equiv \sum_{j=0}^{M-1} a^{jld} \pmod{n_1}.$$

Hence

$$n_1(a^d-1) \mid a^{Md}-1 \text{ if and only if } n_1(a^l-1) \mid a^{Ml}-1.$$

Therefore

$$m = \mathrm{ord}_{n_1(a^d-1)}(a^d)$$

$$= \mathrm{lcm}(\mathrm{lcm}_{p \mid a^d-1}\{\mathrm{ord}_{p^{v_p(n_1)+v_p(a^d-1)}}(a^d)\}\ \mathrm{ord}_t(a^d)).$$

By Lemma A.1. (i)

$$v_p(\mathrm{ord}_{p^{v_p(n_1)+v_p(a^d-1)}}(a^d)) = v_p(n_1) = v_p(sh^{-1}),$$

unless $p=2$, $a^d \equiv 3 \pmod 4$, and $v_2(n_1)>0$ (i.e. s is even) in which case we get

$$2^{1+\max(0, v_2(n_1)-v_2(a^d+1))} = 2^{v_2(sh^{-1})},$$

and so

$$m = \mathrm{lcm}\Big(\prod_{p \mid a^d-1} p^{v_p(sh^{-1})}, u\Big) = \mathrm{lcm}(sh^{-1}, u).$$

Theorem A.3. *We have that*

(i) $m = n_1$ *if and only if* $(p \mid n_1 \Rightarrow p \mid a^d-1)$ *and* $(a^d \equiv 1 \pmod 4$ *or* $v_2(n_1) \leqslant 1)$,

(ii) $m = n_1 - 1$ *if and only if* n_1 *is a prime,* a *is a primitive root* $\pmod{n_1}$, *and* $d = 1$.

Proof. By Lemma A.2, $m = n_1$ if and only if $t = 1$ and $h = 1$, and $m = n_1 - 1$ if and only if $s = 1$ and $\mathrm{ord}_{n_1}(a^d) = n_1 - 1$. The theorem follows easily.

Lemma A.4. *We have that*

(i) $$u = \frac{\mathrm{ord}_t(a)}{\gcd(\mathrm{ord}_t(a), d)} = \frac{\mathrm{ord}_t(a)}{\gcd(\mathrm{ord}_t(a), l)}$$
$$= \frac{\mathrm{lcm}(\mathrm{ord}_t(a), d)}{d} = \frac{\mathrm{lcm}(\mathrm{ord}_t(a), l)}{l}.$$

(ii) $$\mathrm{ord}_t(a) = \mathrm{lcm}\Big(\prod_{p \mid t} p^{\max(0, v_p(t)-z_p)}, \mathrm{ord}_{t_1}(a)\Big),$$

where $z_p = v_p(a^{\mathrm{ord}_{t_1}(a)}-1)$ *and* $t_1 = \prod_{p \mid t} p$.

Proof. We have to prove that

$$\gcd(\mathrm{ord}_r(a), d) = \gcd(\mathrm{ord}_r(a), l).$$

The left hand expression divides the right hand expression. Further

$$\gcd(\mathrm{ord}_r(a), l) \mid \gcd(r, l) = d$$

and

$$\gcd(\mathrm{ord}_r(a), l) \mid \mathrm{ord}_r(a)$$

which shows that equality holds.

(ii) We have

$$\mathrm{ord}_t(a) = \operatorname*{lcm}_{p \mid t}(\mathrm{ord}_{p^{v_p(t)}}(a))$$

$$= \operatorname*{lcm}_{p \mid t}(p^{\max(0, v_p(t) - z_p)} \mathrm{ord}_p(a))$$

$$= \mathrm{lcm}\left(\prod_{p \mid t} p^{\max(0, v_p(t) - z_p)}, \operatorname*{lcm}_{p \mid t}(\mathrm{ord}_p(a))\right).$$

Lemma A.5. *Let p be a prime dividing n_1 and let $n_2 = n_1 p^{-1}$, $r' = \mathrm{ord}_{n_2}(a)$, $d' = \gcd(r', l)$, etc.*

(i) *If $p \mid s$, then $s' = sp^{-1}$, $t' = t$, and $u' = u$.*

(ii) *If $p \mid t$, then $s' = s$ and $t' = tp^{-1}$.*

(iii) *$h' = h/2$ if $p = 2$, $a^d \equiv 3 \pmod 4$ and $1 < v_2(s) \leq v_2(a+1)$*
$= h$ otherwise.

Proof. Let $p_1 \mid n_2$ be a prime. Then $p_1 \mid n_1$, and so $p_1 \mid a^r - 1$ and $p_1 \mid a^{r'} - 1$. Hence $p_1 \mid a^d - 1 = \gcd(a^r - 1, a^t - 1)$ if and only if $p_1 \mid a^{d'} - 1$. (i) and (ii) now follow from the definitions of s' and t' except that $u' = u$ in (i) follows from Lemma A.4.

We divide the proof of (iii) into four cases.

Case I. $v_2(s) \leq 1$. Then $v_2(s') \leq 1$ and so $h' = h = 1$.

Case II. $v_2(s) > 1$ and $a^d \equiv a^{d'} \equiv 1 \pmod 4$. Then $h' = h = 1$.

Case III. $v_2(s) > 1$, $a^d \equiv 1 \pmod 4$, and $a^{d'} \equiv 3 \pmod 4$.

Then d is even, d' is odd, and $a \equiv 3 \pmod 4$. Hence l is even and so r' is odd. Therefore $v_2(s') \leq v_2(a^{r'} - 1) = 1$ and so $h' = h = 1$.

Case IV. $v_2(s) > 1$ and $a^d \equiv 3 \pmod 4$. Since $d' \mid d$, d' is odd also. Hence $v_2(a^d + 1) = v_2(a+1) = v_2(a^{d'} + 1)$. If p is odd, then $v_2(s') = v_2(s)$ and so $h' = h$. If $p = 2$, then $h = 2^{\min(v_2(s), v_2(a+1))-1}$ and $h' = 2^{\min(v_2(s)-1, v_2(a+1))-1}$ and (iii) follows.

Let

$$E = E(n_1) = \{e \mid e \text{ is an integer dividing } n_1 \text{ such that } \mathrm{ord}_{(n_1/e)(a^t-1)}(a^t) = m/e\},$$

Clearly, E is not empty since $1 \in E$. Let

$$E^* = E^*(n_1) = \left\{ e \in E(n_1) \mid \gcd\left(\frac{n_1}{e}, \frac{a^t - 1}{a^{d_0} - 1}\right) = 1 \text{ where } d_0 = \gcd(\mathrm{ord}_{n_1/e}(a), l) \right\}.$$

Theorem A.6. *The set $E^*(n_1)$ is not empty for any n_1.*

Proof. We prove the theorem by induction on n_1. If $n_1 = 1$, then $1 \in E^*(n_1)$. Let $n_1 > 1$ and suppose the assertion is true for all lower values. If $\gcd(n_1, (a^l-1)/(a^d-1)) = 1$, then $1 \in E^*(n_1)$. Otherwise let p be a prime dividing $\gcd(n_1, (a^l-1)/(a^d-1))$. Let n_2, r', etc. be defined as in Lemma A.5. We note

$$p \mid \gcd(n_1, a^l-1) \mid \gcd(a^r-1, a^l-1) = a^d-1.$$

Hence $p \mid s$. By Lemma A.1.(i), $p \mid l/d$ since $v_p(a^l-1) > v_p(a^d-1)$. Therefore $p \nmid r/d$ and so $p \nmid u$ since $u \mid \mathrm{ord}_{n_1}(a^d) = r/d$. We show that $h' = h$. Suppose $h' \neq h$. By Lemma A.5. (iii), $p = 2$, $a \equiv 3 \pmod 4$, d is odd, and $v_2(s) > 1$. Since $s \mid a^r - 1$, r is even, a contradiction since $p = 2 \nmid r/d$. Hence $h' = h$. Since $p \nmid u$ and $u' = u$ we get

$$m' = \mathrm{lcm}(s'h'^{-1}, u') = \mathrm{lcm}(sp^{-1}h^{-1}, u) = p^{-1}m.$$

Hence $p \in E(n_1)$. By the induction hypothesis, there exists an $e' \in E^*(n_2)$. Hence $e'p \in E^*(n_1)$.

Corollary A.7. *We have* $\max E^*(n_1) = \max E(n_1)$.

Proof. Let $e = \max E(n_1)$. By Theorem A.6 there exists an $e' \in E^*(n_1/e)$. Hence $ee' \in E(n_1)$ and so $e' = 1$ by the maximality of e. Therefore $1 \in E^*(n_1/e)$ and so $e \in E^*(n_1)$. Since $E^*(n_1)$ is a subset of $E(n_1)$, $e = \max E^*(n_1)$.

Lemma A.8. (i). *If $e \mid n_1$, then*

$$\mathrm{ord}_{(n_1/e)(a^l-1)}(a^l) \geq m/e.$$

(ii) *If $e \in E(n_1)$ and $e' \mid e$, then $e' \in E(n_1)$.*

Proof. (i) By induction on e. It is true for $e = 1$. Let $e = p$ and let $m' = \mathrm{ord}_{(n_1/p)(a^l-1)}(a^l)$. If $p \mid a^{lm'}-1$, then $m = m'$ or $m = pm'$, otherwise $m = \mathrm{lcm}(m', \mathrm{ord}_p(a^l)) < m'p$. Hence $m' \geq m/p$ in all cases. Finally, suppose e is composite and let $p \mid e$. By the induction hypothesis

$$\mathrm{ord}_{(n_1p^{-1}/ep^{-1})(a^l-1)}(a^l) \geq \frac{1}{ep^{-1}} \mathrm{ord}_{n_1p^{-1}(a^l-1)}(a^l) \geq \frac{1}{ep^{-1}} \cdot \frac{m}{p} = \frac{m}{e}.$$

(ii) By (i) and $e \in E(n_1)$ we get

$$\frac{m}{e} = \mathrm{ord}_{(n_1e'^{-1}/ee'^{-1})(a^l-1)}(a^l) \geq \frac{1}{ee'^{-1}} \mathrm{ord}_{n_1e'^{-1}(a^l-1)}(a^l) \geq \frac{e'}{e} \cdot \frac{m}{e'} = \frac{m}{e}.$$

Hence we have equality and so $e' \in E(n_1)$.

Let $t_1 = \prod_{p \mid t} p$ and define ε_s and ε_t by

$$v_p(\varepsilon_s) = \max(0, v_p(s) - v_p(u)) \qquad \text{if } p \neq 2 \text{ or } h = 1,$$

$$= \max(0, \min(v_2(sh^{-1}) - v_2(u), v_2(s) - v_2(a+1)) \qquad \text{if } p = 2 \text{ and } h > 1,$$

$$v_p(\varepsilon_t) = \max(0, v_p(t) - z_p - \max(v_p(d), v_p(\operatorname{ord}_{n_1}(a)))) \qquad \text{for all } p.$$

Theorem A.9. *Let $e_0 = \varepsilon_s\varepsilon_t$. We have $e \in E(n_1)$ if and only if $e \mid \varepsilon_s\varepsilon_t$. In particular* $\max E^*(n_1) = \max E(n_1) = e_0$.

Lemma A.10. *Let $u_1 = \operatorname{ord}_{n_1}(a^d)$. Then*

(i) $u_1 = \operatorname{ord}_{t/\varepsilon_t}(a^d)$,

(ii) $\varepsilon_t = \dfrac{u}{u_1}$,

(iii) $t_1 \mid t/\varepsilon_t$.

Proofs. For $e \mid n_1$, let $e_s = \prod_{p \mid s} p^{v_p(e)}$ and $e_t = \prod_{p \mid t} p^{v_p(e)}$. Further, let $n_1' = n_1/e$, $r' = \operatorname{ord}_{n_1'}(a)$, etc. From Lemma A.5 we get by induction that $s' = s/e_s$ and $t' = t/e_t$. Hence by Lemma A.2, $e \in E(n_1)$ if and only if

$$\operatorname{lcm}\left(\frac{s}{e_s}h'^{-1}, u'\right) = \frac{1}{e_s e_t}\operatorname{lcm}(sh^{-1}, u). \tag{A.1}$$

First we show that if $e \in E(n_1)$, then $e \mid \varepsilon_s\varepsilon_t$. By Lemma A.8 (ii), $p^{v_p(e)} \in E(n_1)$. Hence what we have to show is that if $p^\delta \in E(n_1)$, then $p^\delta \mid \varepsilon_s\varepsilon_t$. First, let $e = p^\delta \in E(n_1)$, where $p \mid s$ and $\delta > 0$. By Lemma A.5 (i) $u' = u$. Hence, by (1) we get

$$\max(v_p(sh'^{-1}) - \delta, v_p(u)) = \max(v_p(sh^{-1}), v_p(u)) - \delta.$$

Since $h' \mid h$ we have $v_p(sh'^{-1}) \geq v_p(sh^{-1})$. Hence we must have $v_p(h') = v_p(h)$ and $v_p(sh^{-1}) - \delta \geq v_p(u)$. If $p \neq 2$ or $h = 1$, then $v_t(h') = v_p(h) = 0$. If $p = 2$ and $h > 1$, then by Lemma A.5 (iii), $v_2(h') = v_2(h)$ only if $v_2(s) - \delta \geq v_2(a+1)$. Hence we get $\delta \leq v_p(\varepsilon_s)$ in both cases. Next, let $e = p^\delta \in E(n_1)$ where $p \mid t$ and $\delta > 0$. By (A.1), we get

$$v_p(u') = v_t(u) - \delta.$$

By Lemma A.4, this is possible only if

$$v_p(t) - \delta - z_p \geq \max(v_p(l), v_p(\operatorname{ord}_t(a)))$$

$$\geq \max(v_p(d), v_p(\operatorname{ord}_{n_1}(a)))$$

and so $\delta \leq v_p(\varepsilon_t)$. This proves that if $e \in E(n_1)$, then $e \mid \varepsilon_s\varepsilon_t$. We go on to prove the converse and Lemma A.10. Let $e_0 = \varepsilon_s\varepsilon_t$. Since $v_p(\varepsilon_t) < v_p(t)$ when $v_p(t) > 0$ we see that $t_1' = t_1$ and $t_1 \mid (t/\varepsilon_t)$ which proves (iii). Furthe

$$u' = \frac{\operatorname{lcm}\left(\prod_{p|t} p^{\max(0, v_p(t)-v_p(\varepsilon_t)-z_p)}, \operatorname{ord}_{t_1}(a), l\right)}{l}.$$

If $v_p(\varepsilon_t) = 0$, then clearly $v_p(u) = v_p(u')$. If $v_p(\varepsilon_t) > 0$ we show that $v_p(l) = v_p(d)$. Since

$$\operatorname{ord}_s(a) \mid d \operatorname{ord}_s(a^d) = dsh^{-1}$$

we get

$$v_p(\operatorname{ord}_s(a)) \leqslant v_p(d) < v_p(t) - z_p = v_p(\operatorname{ord}_t(a)).$$

Since $r = \operatorname{lcm}(\operatorname{ord}_s(a), \operatorname{ord}_t(a))$ and $d = \gcd(r, l)$ this implies that $v_p(l) = v_p(d)$. Hence $v_p(u') = v_p(u) - v_p(\varepsilon_t)$. This proves that $u' = u/\varepsilon_t$. Further

$$v_p(t) - z_p - v_p(\varepsilon_t) = \max(v_p(\operatorname{ord}_{t_1}(a)), v_p(l))$$

and we get, by Lemma A.4,

$$\operatorname{ord}_{t/\varepsilon_t}(a^d) = \frac{\operatorname{lcm}(\operatorname{ord}_{t_1}(a), l)}{l} = u_1.$$

This proves (i) and (ii). Next we see that $h' = h$. It follows that (A.1) is satisfied, i.e. that $e \in E(n_1)$. In general, if $e \mid \varepsilon_s\varepsilon_t$, then $e \in E(n_1)$ by Lemma A.8 (ii).

We next find necessary and sufficient conditions for $m/e_0 = 2$ or $m/e_0 = (n_1/e_0) - 1$.

Note that we have by Lemma A.4 and Lemma A.10

$$u' = \operatorname{ord}_{t'}(a^d) = \operatorname{ord}_{t'}(a^d) = \operatorname{ord}_{t_1}(a^d) = u_1$$

where u', d' etc. refer to $n_1' = n_1/e_0$.

Theorem A.11. *We have that $m' = 2$ if and only if the following conditions hold.*

(i) *If $p \mid t$, then $p \mid a^d + 1$.*

(ii) *If $t = 1$, then $a^d \equiv 3 \pmod 4$ and $v_2(s) > 1$.*

Proof. Suppose $m' = 2$. Let $p \mid t$ and $p \nmid a^d + 1$. Since $p \nmid a^d + 1$ and $p \nmid a^d - 1$ we have $p \nmid a^{2d} - 1$. Therefore we have by Lemma A.2 and Lemma A.10

$$m' \geqslant u' \geqslant \operatorname{ord}_{t_1}(a^d) \geqslant \operatorname{ord}_p(a^d) > 2$$

which contradicts that $m' = 2$. Hence (i) is proved.

Let $t = 1$. Suppose $a^d \not\equiv 3 \pmod 4$ or $v_2(s) \leqslant 1$. Then $u = h = 1$ and therefore $v_p(\varepsilon_s) = v_p(s)$ for all p. Hence $\varepsilon_s = s$ and

$$m' = \operatorname{lcm}\left(\frac{s}{e_s}, u'\right) = 1$$

a contradiction. Hence (ii) is proved.

Suppose (i) and (ii) hold. Note that

$$u = 2\prod_{p_i \mid t} p^{v_{p_i}(n_1) - z^*_{p_i}}$$

where

$$z^*_{p_i} = v_{p_i}(a^{d \operatorname{ord}_{p_i}(a^d)} - 1) = z_{p_i} + v_{p_i}(d).$$

It is sufficient to show that

$$v_p(e_0) = v_p(m) \quad \text{when } p \mid n_1,\ p \text{ odd},$$

and

$$v_2(e_0) = v_2(m) - 1.$$

Let $p \mid s$, p odd. Then $v_p(u) = 0$ and we get by definition and by Lemma A.2

$$v_p(m) = \max(v_p(s), v_p(u)) = v_p(e_0).$$

Let $p \mid t$. By definition and by Lemma A.2,

$$\begin{aligned} v_p(m) &= \max(v_p(s), v_p(u)) \\ &= \max(v_p(\operatorname{ord}_{p^{v_p(t)}}(a^d)), v_p(\operatorname{ord}_{p^{v_p(t)}}(a^d))) \\ &= \max(0, v_p(t) - z_p - v_p(d)). \end{aligned}$$

Since

$$\operatorname{ord}_{t_1}(a^d) = \frac{\operatorname{ord}_{t_1}(a)}{\gcd(\operatorname{ord}_{t_1}(a), d)} \Big| 2$$

we have $v_p(d) \geq v_p(\operatorname{ord}_{t_1}(a))$. Hence $v_p(m) = v_p(e_0)$. Let $p = 2$. If $t > 1$ then $v_2(u) = 1$ and we get by straightforward calculations that $v_2(e_0) = v_2(m) - 1$ in all cases. If $t = 1$, then $u = 1$, $a^d \equiv 3 \pmod 4$, and $v_2(s) > 1$ which also give $v_2(e_0) = v_2(m) - 1$.

Theorem A.12. *We have that $m' = n'_1 - 1$ if and only if the following conditions hold,*

(i) $t = p^i$ *for some* $i > 0$,
(ii) $\operatorname{ord}_p(a^d) = p - 1$,
(iii) $i = 1$ *or* $z_p + v_p(d) = 1$,
(iv) $\gcd(s, p - 1) = 1$.

Proof. Suppose $m' = n'_1 - 1$. Since $s'h'^{-1} \mid \gcd(m', n'_1) = 1$ we have $s' = 1$. If $t = 1$, then $t' = 1$. Hence $n'_1 = 1$ and $m' = 0$, a contradiction. If $t = pt_2$ where $t_2 > 1$, and there exists a prime $p_2 \neq p$ which divides t_2, then

$$u' = u_1 = \operatorname{ord}_{t_1}(a^d) < t_1 - 1,$$

since t_1 is composite. By Lemma A.10 and Lemma A.2 we have

$$m' \leq \operatorname{lcm}(s', u') < s't_1 - 1 \leq n'_1 - 1.$$

This proves (i).

If $\mathrm{ord}_p(a^d) < p-1$, then $u_1 < p-1$ and as above we get $m' < n_1' - 1$, a contradiction. Hence (ii) is proved.

If (iii) does not hold, then

$$\begin{aligned} v_p(t') &= v_p(t) - v_p(\varepsilon_1), \\ &= \min(v_p(t), z_p + \max(v_p(d), v_p(\mathrm{ord}_{n_1}(a)))), \\ &= \min(i, z_p + v_p(d)), \\ &> 1. \end{aligned}$$

Therefore $t' > p$. Since $s' = 1$ we have $m' = u' = p-1$ by Lemma A.10 and Lemma A.2. This proves (iii) since $n_1' - 1 > p - 1 = m'$.

If $\gcd(s, p-1) > 1$, then by definition $v_{p_1}(\varepsilon_s) < v_{p_1}(s)$ when $p_1 \mid \gcd(s, p-1)$. Hence $s' > 1$, a contradiction and (iv) is proved.

Suppose that (i)–(iv) hold. Then by (i) and (iii) we have $t' = p$. From (ii) and Lemma A.10 we get $u' = p-1$. Since $\gcd(s, p-1) = 1$ we have that s is odd and therefore by definition $\varepsilon_s = s$. Therefore $s' = 1$. This gives

$$m' = \mathrm{lcm}(s'h'^{-1}, u') = p - 1 = s't' - 1$$

which was to be proved.

References

[1] L.D. Baumert and R.J. McEliece, Weights of irreducible cyclic codes, Information and Control 20 (1972) 158–175.

[2] L.D. Baumert and J. Mykkeltveit, Weights distributions of some irreducible cyclic codes, DSN progress Report 16 (1973) 128–131 (published by Jet Propulsion Laboratory, Pasadena, California).

[3] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, NY, 1968).

[4] P. Delsarte and J.-M. Goethals, Irreducible cyclic codes of even dimension, in: Proc. 2nd Chapel Hill Conference on Combinatorial Math. and Appl. (Univ. North Carolina Press, Chapel Hill, NC, 1970).

[5] R.J. McEliece, A class of two-weight codes, Jet Propulsion Laboratory Space Programs Summary 37-41, Vol IV, 264–266.

[6] R.J. McEliece, Irreducible cyclic codes and Gauss sums, in: M. Hall Jr. and J.H. van Lint, eds., Combinatorics, Part I (Mathematical Centre Tracts 55, Mathematish Centrum, Amsterdam, 1974).

[7] R.J. McEliece and H. Rumsey Jr., Euler products, cyclotomy, and coding, J. Number Theory 4 (1972) 302–311.

[8] J.M. Goethals, Factorization of cyclic codes, IEEE Trans. Information Theory, IT-13 (April 1967) 242–246.

[9] Jay Goldman and Gian-Carlo Rota, The number of subspaces of a vector space, in: W T. Tutte, ed., Recent Progress in Combinatorics (Academic Press, NY, 1969).

[10] S.S. Oganesian, V.G. Yagdzyan and V.J. Tairyan, On a class of optimal cyclic codes, in: B.N. Petrov and F. Csáki, eds., 2nd International Symposium on Information theory (Akadémiai Kiadó, Budapest, 1973).

[11] J.H. Van Lint, Coding Theory (Lecture Notes in Mathematics 201, Springer-Verlag, Berlin, 1971).

[12] John Riordan, Combinatorial Identities (John Wiley, London, 1968).